**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | | |
|---|---|---|---|
| Appl. No. | : | **10/066,251** | Confirmation No. **2791** |
| Applicant | : | **Richard L. Hammons** | |
| Filed | : | **January 31, 2002** | |
| TC/A.U. | : | **2434** | |
| Examiner | : | **Andrew L. Nalven** | |
| Docket No. | : | **112-0020US** | |
| Customer No. | : | **29855** | |
| Title | : | **NETWORK SECURITY THROUGH CONFIGURATION SERVERS IN THE FABRIC ENVIRONMENT** | |

Box Appeal Brief
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Mail Stop: Appeal Briefs – Patents

## APPEAL BRIEF

## TABLE OF CONTENTS

## I. REAL PARTY IN INTEREST

The real party in interest is Brocade Communications Systems, Inc.

## II. RELATED APPEALS AND INTERFERENCES

None.

## III. STATUS OF CLAIMS

Claims 1–29 and 54 are rejected and are appealed. Claims 30–53 were subject to a restriction requirement, and have been cancelled. (It is noted that these claims are pending in various divisional applications.)

## IV. STATUS OF AMENDMENTS

None filed

## V. SUMMARY OF CLAIMED SUBJECT MATTER

This section provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by paragraph and line number and to the drawings by reference characters as required by 37 CFR § 41.37(c)(l)(v). Where applicable, each element of the claims is identified with a corresponding reference to the specification and drawings. Citation to the specification and/or drawings does not imply that limitations from the specification and drawings should be read into the corresponding claim element. Additionally, references are not necessarily exhaustive, and various claim elements may also be described at other locations.

Independent claim 1 recites network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network (¶ 0080, ll. 1–13; Fig. 10, element 1022). The claim further recites:

- that the secure network comprises a plurality of switching devices (Fig. 10, elements 1001–06); and
- that the set of management functions comprises the recognition, operation and succession of the network configuration entity (¶ 0080, ll. 7–8).

Dependent claim 2 depends from claim 1 and further recites that the network configuration entity include:

- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity (¶ 0083, ll. 2–4; Figs 11a, 11b & 11c).

Dependent claim 5 depends (indirectly) from claim 1 and further recites that the network configuration entity includes:

- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing a DCC list, said DCC list associated with said one or more rules for interaction between and among devices and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network (¶ 0126–¶ 0130).

Dependent claim 6 depends (indirectly) from claim 1 and further recites that the network configuration entity includes:

- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing a DCC list, said DCC list associated with said one or more rules for interaction between and among devices and comprising definitions that logically bind each port in said secure network to one or more other ports resident in said network (¶ 0126–¶ 0130).

Dependent claim 10 depends (indirectly) from claim 1 and further recites that the network configuration entity includes:

- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing an MAC list, said MAC list comprising an indication of network endpoints from which management access is acceptable (¶ 0113–¶ 0123).

Independent claim 17 recites a network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network (¶ 0080,

ll. 1–13; Fig. 10, element 1022), said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity (¶ 0080, ll. 7–8), (ii) switch connection controls for designating devices to participate in the secure network (¶ 0080, ll. 8–9), (iii) device connection controls that indicate port relationships in said secure network (¶ 0080, ll. 9–10), and (iv) management access controls that restrict management services to a defined set of endpoints (¶ 0080, ll. 10–11), said network configuration entity comprising:

- a processor (Fig. 2, element 202); and
- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing
    - an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity (¶ 0083, ll. 2–4; Figs 11a, 11b & 11c),
    - an SCC list, said SCC list comprising an indication of each device allowed to participate in said secure network (¶ 0131–¶ 0133),
    - a DCC list, said DCC list associated with said one or more rules for interaction between and among devices and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network (¶ 0126–¶ 0130), and
    - a MAC list, said MAC list comprising an indication of network endpoints from which management access is acceptable (¶ 0113–¶ 0123).

Independent claim 18 recites a Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity (¶ 0080, ll. 1–13; ¶ 0082, ll. 4–7), said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity (¶ 0080, ll. 7–8), (ii) switch connection controls for designating devices to participate in the secure network (¶ 0080, ll. 8–9), (iii) device connection controls that indicate port relationships in said secure network (¶ 0080, ll. 9–10), and (iv) management access controls that

restrict management services to a defined set of endpoints (¶ 0080, ll. 10–11), the Fibre Channel switching device comprising:

- a processor (Fig. 2, element 202); and
- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing
  - an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity (¶ 0083, ll. 2–4; Figs 11a, 11b & 11c),
  - an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network (¶ 0131–¶ 0133),
  - a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network (¶ 0126–¶ 0130), and
  - a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable (¶ 0113–¶ 0123).

Independent claim 19 recites a Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity (¶ 0080, ll. 1–13; ¶ 0082, ll. 4–7), said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity (¶ 0080, ll. 7–8), and (ii) switch connection controls for designating devices to participate in the secure network (¶ 0080, ll. 8–9), the Fibre Channel switching device comprising:

- a processor (Fig. 2, element 202); and
- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing
  - an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an

indication of each device in the network that may operate as said network configuration entity (¶ 0083, ll. 2–4; Figs 11a, 11b & 11c), and

- an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network (¶ 0131–¶ 0133).

Independent claim 20 recites a Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity (¶ 0080, ll. 1–13; ¶ 0082, ll. 4–7), said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity (¶ 0080, ll. 7–8), and (ii) device connection controls that indicate port relationships in said secure network (¶ 0080, ll. 9–10), said Fibre Channel switching device comprising:

- a processor (Fig. 2, element 202); and
- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing
  - an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity, and
  - a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network (¶ 0126–¶ 0130).

Independent claim 21 recites a Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity (¶ 0080, ll. 1–13; ¶ 0082, ll. 4–7), said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration

entity (¶ 0080, ll. 7–8), and (ii) management access controls that restrict management services to a defined set of endpoints (¶ 0080, ll. 10–11), said Fibre Channel switching device comprising:

- a processor (Fig. 2, element 202); and
- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing
  - an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity (¶ 0083, ll. 2–4; Figs 11a, 11b & 11c), and
  - a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable (¶ 0113–¶ 0123).

Independent claim 22 recites a Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity (¶ 0080, ll. 1–13; ¶ 0082, ll. 4–7), said secure network comprising a plurality of switching devices, said set of management functions comprising (i) switch connection controls for designating devices to participate in the secure network (¶ 0080, ll. 8–9), and (ii) device connection controls that indicate port relationships in said secure network, said Fibre Channel switching device comprising (¶ 0080, ll. 9–10):

- a processor (Fig. 2, element 202); and
- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing
  - an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network (¶ 0131–¶ 0133), and
  - a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network (¶ 0126–¶ 0130).

Independent claim 23 recites a Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity (¶ 0080, ll. 1–13; ¶ 0082, ll. 4–7), said secure network comprising a plurality of switching devices, said set of management functions comprising (i) switch connection controls for designating devices to participate in the secure network (¶ 0080, ll. 8–9), and (ii) management access controls that restrict management services to a defined set of endpoints (¶ 0080, ll. 10–11), said Fibre Channel switching device comprising:

- a processor (Fig. 2, element 202); and
- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing
    - an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network (¶ 0131–¶ 0133), and
    - a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable (¶ 0113–¶ 0123).

Independent claim 24 recites a Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity (¶ 0080, ll. 1–13; ¶ 0082, ll. 4–7), said secure network comprising a plurality of switching devices, said set of management functions comprising (i) device connection controls that indicate port relationships in said secure network (¶ 0080, ll. 9–10), and (ii) management access controls that restrict management services to a defined set of endpoints (¶ 0080, ll. 10–11), said Fibre Channel switching device comprising:

- a processor (Fig. 2, element 202); and
- a memory (¶ 0058, ll. 7–9; Fig. 2, elements 208, 210) for storing
    - a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network

configuration entity, to one or more other ports resident in the secure network (¶ 0126–¶ 0130), and

- a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable (¶ 0113–¶ 0123).

Independent claim 25 recites a network comprising a network configuration entity and one or more other entities (Fig. 10), said network configuration entity having network-wide control over a defined set of management functions (¶ 0080, ll. 1–13), said set of management functions comprising:

- the recognition, operation and succession of the network configuration entity (¶ 0080, ll. 7–8);
- one or more rules for interaction between and among entities in the network (¶ 0080, ll. 8–9);
- one or more rules governing management level access to the network (¶ 0080, ll. 10–11); and
- one or more rules governing management level access to one or more entities (¶ 0093).

Dependent claim 26 depends from claim 25 and further recites that:

- said function of recognition, operation and succession of the network configuration entity is associated with a list of network devices that are eligible to become equivalent to said network configuration entity (¶ 0083, ll. 2–4; Figs 11a, 11b & 11c).

Dependent claim 27 depends from claim 25 and further recites that:

- the network configuration entity has exclusive control over one or more of said management functions (¶ 0080, ll. 11–13).

Dependent claim 28 depends from claim 25 and further recites that the network:

- further comprises one or more back-up network configuration entities (¶ 0082, ll. 1–6).

Dependent claim 29 depends from claim 25 and further recites that:

- each of said security and management functions corresponds with a data structure in a memory (¶ 0113–¶ 1033).

Independent claim 54 is drawn to a method of securing a network having a Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management function is controlled throughout said secure network by a network configuration entity, said method comprising the steps of:

- controlling the recognition, operation and succession of the network configuration entity by designating an NCE list comprising an indication of each device in the network that may operate as said network configuration entity (¶ 0080, ll. 7–8; ¶ 0083, ll. 2–4);
- designating a unique name for each devices that may participate in the secure network (¶ 0080, ll. 8–9; ¶ 0131–¶ 0133);
- indicating port relationships in said secure network to specifically delineate a list of unique names for ports that any given port may communicate with (¶ 0080, ll. 9–10; ¶ 0126–¶ 0130); and
- restricting management access to a pre-defined set of access methods (¶ 0080, ll. 10–11; ¶ 0113–¶ 0123).

## VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1–9, 11–16, and 25–29 were rejected under 35 U.S.C. § 103(a) as obvious over U.S. Pre-Grant Publication 2003/0208589 to Yamamoto et al. ("Yamamoto") in view of U.S. Pre-Grant Publication 2002/0174207 to Battou ("Battou"). Claims 10, 17–24, and 54 were rejected under 35 U.S.C. § 103(a) as obvious over Yamamoto and Battou in further view of U.S.

Pre-Grant Publication 2004/0015957 to Zara et al. ("Zara"). Review of these rejections is sought as follows:

1. The rejection of claims 1 and 25–29 as obvious over Yamamoto in view of Battou is improper, and review of this rejection is sought.

2. The rejection of claim 2 as obvious over Yamamoto in view of Battou is improper, and review of this rejection is sought.

3. The rejection of claims 5 and 6 as obvious over Yamamoto in view of Battou is improper, and review of this rejection is sought.

4. The rejection of claim 16 as obvious over Yamamoto in view of Battou is improper, and review of this rejection is sought.

5. The rejection of claims 10, 17–24 and 54 as obvious over Yamamoto in view of Battou in further view of Zara is improper, and review of this rejection is sought.

## VII. ARGUMENT

The claims do not stand or fall together. Instead, Appellants present separate arguments for various independent and dependent claims. After a concise discussion of cited art, each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 CFR § 41.37(c)(l)(vii). To aid in review of the Office Action, certain rejections have been copied into this brief. Arguments as to the rejection then follow.

### A. The Rejection Of Claims 1 And 25–29 As Obvious Over Yamamoto In View Of Battou Is Improper

As noted above, claims 1 and 25–29 were rejected under 35 U.S.C. § 103(a) as obvious over Yamamoto in view of Battou. Specifically, these claims were rejected as follows:

> 8. **With regards to claims 1, 25-29**, Yamamoto teaches a network configuration entity configured or adapted to exclusively control a defined set of management functions through a secure network (Yamamoto, paragraph 0059), said secured network comprising a plurality of switching devices (Yamamoto, paragraph 0001), and set said of management functions comprising recognition and operation (Yamamoto, paragraphs 0119, 0128). Yamamoto fails to teach the management functions including succession. However, Battou teaches the management functions including succession (Battou, page 1 paragraph 0008). At the time the invention was made, it would have been obvious to one of ordinary skill in the art to utilize Battou's method of succession for management servers because it offers the advantage of improving the viability of the network by providing a greater degree of fault tolerance thus ensuring that network remains available in the event of a management server failure (Battou, paragraphs 0005-0007)

Final Rejection at pp. 4–5. This rejection is improper for at least the reasons set forth below.

Yamamoto relates to methods for identifying configuration inconsistencies in a Fibre Channel network. *See* Yamamoto at Abstract. Brief inspection of Yamamoto suggests that the system of Yamamoto operates by collecting information about a Fibre Channel network into a variety of tables and checking these tables for inconsistencies that would render the network inoperative. *See id.* at ¶¶ [0119]–[0161].

Battou has nothing at all to do with Fibre Channel Networks. Battou relates to network management systems that include distributed network managers have responsibility for certain portions of the network. *See* Battou at Abstract. The network managers can detect when another network manager is not functioning correctly, and can, without operator intervention, elect one of themselves to take over the functions of the malfunctioning/non-functioning counterpart. *See id.* Moreover, the system of Battou contemplates that the management network is a separate, out-of-band network from the underlying communications network. *Id.* at ¶¶ [0002]–[0004].

Conversely, Claim 1 is drawn to a network configuration entity that is "configured or adapted to exclusively control a defined set of management functions throughout a secure network" where the set of management functions includes "the recognition, operation and succession of the network configuration entity." The rejection set forth above parses the words of claim 1 so finely as to eviscerate the limitation. As noted above, claim 1 requires that the

network configuration entity "exclusively control a defined set of management functions throughout a secure network" and that the set of management functions include "recognition, operation and succession of the network configuration entity." Thus, the claim requires that a network configuration entity *exclusively* control three things—(1) recognition of the network configuration entity, (2) operation of the network configuration entity, and (3) succession of the network configuration entity—throughout the secure network.

Examiner concedes that "Yamamoto fails to teach the management functions including succession." Final Rejection at p. 4. While this statement is certainly true, the limitation of claim 1 missing from Yamamoto is not merely succession of the network configuration entity, but rather *exclusive* control of succession of the network control entity throughout the network. This renders Examiner's reliance on Battou for this teaching inappropriate. Battou does not teach that any entity has exclusive control of succession throughout the network. Rather, Battou teaches exactly the opposite, namely that a plurality of devices share control over recognition, operation and succession of the network configuration entity.

For example, at paragraph [0008] Battou describes "a hierarchical network management system in which a plurality of NMS managers, each responsible for different portions or aggregations of a communications network, are logically arranged in a tree structure." The fact that there are multiple NMS managers, each responsible for different portions of the network completely negates the contention that any one of these devices maintains exclusive control over the required parameters. Battou goes on to explain that: "The NMS managers within each sub-group monitor the status of one another in order to detect when one of them is no longer operational. If this happens, the remaining operational NMS managers of the sub-group collectively elect one of them to assume the responsibility of the non-operational NMS manager." Collectively deciding upon an order of succession for a failed network component is antithetical to claim 1, which requires that the network configuration entity maintain exclusive control over, among other things, "succession of the network configuration entity."

In summary, Battou may teach succession of control entities, but Battou clearly teaches exactly the opposite of exclusive control (*i.e.*, shared control). Therefore, the combination of Yamamoto (which teaches control of things other than "succession of the network entity") and Battou (which, at most, teaches shared control of "succession of the network entity") fails to

teach or suggest each limitation of claim 1. Therefore, the rejection of claim 1 as obvious over Yamamoto in view of Battou is improper.

Moreover, the combination of Yamamoto with Battou is inappropriate. Yamamoto relates to Fibre Channel networking, while Battou relates to out-of-band management networks for communication networks. Because of the drastic differences between these types of networks, Examiner's statement that it would have been obvious to combine Battou with Yamamoto is merely a self-serving conclusion and not an articulated reason why one of ordinary skill in the art would have combined these two fundamentally different technologies. Besides, the combination of Battou with Yamamoto is clearly improper in view of the fact that Battou's disclosure of shared, distributed control teaches away from exclusive control, as recited in claim 1. The lack of an articulated reason that one of ordinary skill in the art would combine the teachings of Battou with Yamamoto provides a separate, independent reason why the rejection of claim 1 is improper.

The Examiner's response to these arguments, presented at p. 2 of the Final Rejection, do not provide any rebuttal of these arguments. Examiner concedes that Battou merely teaches management control of succession (clearly leaving out the recitation in the claim that the control of succession be "exclusive"). Examiner further fails to address the lack of any articulated reason why one of ordinary skill in the art would combine the disparate Battou and Yamamoto references. Thus, the Examiner's response provides no reason why the rejection of claim 1 should not be reversed as improper.

As can be seen from Examiner's rejection of claim 1 (reproduced above), independent claim 25 and claims 26–29 depending therefrom were rejected using exactly the same rationale as the rejection of claim 1. Despite the fact that claim 25 is a separate independent claim having different limitations than claim 1, Examiner has failed to provide any separate analysis of claim 25. Nonetheless, the rejection of claim 25 is improper for at least the reasons set forth above with respect to claim 1.

More specifically, claim 25 recites a network comprising "a network configuration entity that has network-wide control over a defined set of management functions" including "the recognition, operation *and succession of the network configuration entity*..." (emphasis added). As described in greater detail above, the Examiner has conceded that Yamamoto has no teaching

or suggestion at all relating to the control of succession of the network configuration entity. Furthermore, Battou contains no teaching or suggestion of any device that has network-wide control over anything—including succession of the network configuration entity." Moreover, Examiner's rejection of claim 25 provides no articulation of any reason why one of ordinary skill in the art would combine Yamamoto with Battou. Therefore, the rejection of claim 25 is improper for essentially the same reasons set forth above with respect to claim 1 and should, therefore, be reversed.

While Examiner has not specifically addressed claim 26, which depends from claim 25, claim 26 is separately patentable over Yamamoto and Battou. Claim 26 recites that in the network of claim 25 "recognition, operation and succession of the network configuration entity is associated with a list of network devices that are eligible to become equivalent to said network configuration entity." Examiner has provided no citation to any reference teaching this limitation. Moreover, neither reference includes any such teaching. Thus, the rejection of claim 28 is improper and should be reversed.

Similarly, Examiner has not specifically addressed claim 28, which also depends from claim 25. Claim 28 is also separately patentable over Yamamoto and Battou. Claim 28 recites that the network of claim 25 further comprises "one or more back-up network configuration entities." Yamamoto clearly lacks any such teaching. While the Examiner contends that Battou teaches succession of certain network entities, these are not "network configuration entities" as required by claim 28 because the entities of Battou do not have "network-wide" control. Thus, the rejection of claim 28 is also improper and should be reversed.

### B. The Rejection Of Claim 2 As Obvious Over Yamamoto In View Of Battou Is Improper

Claim 2 depends from claim 1 and further recites that the network configuration entity of claim 1 include a memory for storing an NCE list "comprising an indication of each device in the network that may operate as said network configuration entity." Examiner implicitly concedes that Yamamoto contains no such teaching, as he relies on Battou at ¶¶ [0268]–[0271], reproduced below:

> [0268] Each NMS includes software that runs separate and apart from the network it controls, as well as NMS agent software that runs on each Node Manager of the NMS's network. The NMS agent software allows the each NMS to communicate with the Node Managers of each of its network's nodes.
>
> [0269] Moreover, each NMS may use a database server to store persistent data, e.g., longer-life data such as configuration and connection information. The database server may use LDAP, and Oracle® database software to store longer-life data such as configuration and connection information.
>
> [0270] LDAP is an open industry standard solution that makes use of TCP/IP, thus enabling wide deployment. Additionally, a LDAP server can be accessed using a web-based client, which is built into many browsers, including the Microsoft Explorer® and Netscape Navigator® browsers. The data can be stored in a separate database for each instance of a network, or multiple networks can share a common database server depending on the size of the network or networks. As an example, separate databases can be provided for each of networks A, B and C, where each database contains information for the associated network, such as connection, configuration, fault, and performance information. In addition, the root NMS (e.g., NMS 3015) can be provided with a summary view of the status and performance data for Networks B and C.
>
> [0271] The hierarchical NMS structure is incorporated into the control architecture as needed.

Responding to the Examiner's rejection in any significant detail is virtually impossible, as nothing in these cited paragraphs describes anything even resembling an NCE list "comprising an indication of each device in the network that may operate as said network configuration entity," nor has the Examiner indicated what portions of this passage meet the cited limitation. Examiner response to this argument at p. 3 of the final rejection provides no further citation, explanation, or analysis. Therefore, the rejection of claim 2 is improper and should be reversed.

### C. The Rejection Of Claims 5 And 6 As Obvious Over Yamamoto In View Of Battou Is Improper

Claims 5 and 6 depend (indirectly) from claim 1 and further recite that the network configuration entity includes a memory for storing a DCC list "associated with said one or more rules for interaction between and among devices...." Examiner cites Yamamoto at Fig. 11 and ¶ [0042] as teaching this limitation. Figure 11 of Yamamoto is a diagram of a "Topology Table," which is described at ¶¶ [0105]–[0112]. Review of this passage shows that the topology table is created by the SAN manager by combining various other tables. Nothing in this passage

(or Fig. 11) suggests that the information contained in the topology table is "associated with said one or more rules for interaction between and among devices...." Moreover, ¶ [0042] cited by Examiner has nothing to do with Fig. 11, and instead describes basic information about Fibre Channel zoning. Again, nothing in this passage has anything to do with "one or more rules for interaction between and among devices...." Examiner's recitation of conventional Fibre Channel zoning (as described in the cited ¶ [0042]) does not provide any additional justification for the rejection of claims 5 and 6, as the cited references plainly fail to teach the relevant limitation, or even anything similar to the relevant limitation. Therefore, the rejections of claims 5 and 6 are improper and should be reversed.

### D. The Rejection Of Claim 16 As Obvious Over Yamamoto In View Of Battou Is Improper

Claim 16 depends (indirectly) from claim 1 and further recites that the network configuration entity of claim 1 include a memory for storing an SCC list "comprising a list of devices authorized to participate in said secure network." Examiner cites two paragraphs of Yamamoto (¶¶ [0001], [0096], [0098], & [0120]) and three paragraphs of Battou (¶¶ [0302] & [0306]–[0307]) as teaching the required SCC list. Each of these passages is reproduced below, with comments following:

> **[0001]** The present invention relates generally to storage networks, and more particularly to techniques for centralized configuration management for servers, switches, and disk subsystems in storage networks.

As can be plainly seen, ¶ [0001] of Yamamoto says nothing at all about an SCC list "comprising a list of devices authorized to participate in said secure network."

> [0096] **FIGS. 9*a*-9*b*** illustrate representative LUN Masking Tables (**13130*a*** and **13130*b***) in a specific embodiment of the present invention. These tables provide the information of the LUN Masking configuration in a disk subsystem. These tables are the permission list for each LUN in a SAN. When IT administrators specify the LUN to be accessed or not to be accessed by the specified host port, Management Agent **13100** stores the LUN Masking configuration in these tables. In a specific embodiment, these tables comprise columns for a host port ID (**910**) and an LUN masking configuration list (**920**).
>
> [0098] LUN Masking Configuration List (**920**) is a List of permission settings for each binding in a server. This column has several sub-columns, each of which is specified to the binding. If the specified host port can access the specified binding LU, the value of its sub-column in the list is "OK". If not, the value is "NG".

Again, ¶¶ [0096] and [0098] of Yamamoto say nothing at all about an SCC list "comprising a list of devices authorized to participate in said secure network." At most these passages teach a LUN (Logical Unit Number) masking table, which describe whether specific host ports are allowed to access certain portions of the network. This is not the same thing as a list of devices authorized to participate in the secure network.

> [0120] The SAN Manager **14000** discovers the SAN devices based on the Discovery List **14110**, and SAN Manager **14000** collects the configuration information from the Management Agent in a SAN device. [Step **1310**] The SAN Manager **14000** stores all the configuration information in the Topology Repository **14120**. If any updates exist, the SAN Manager **14000** stores the old configuration in the Configuration History Table **14140**. [Step **1320**] The SAN Manager **14000** makes or updates the Topology Table **14130** based on the Topology Repository **14120**. [Step **1330**] Then, the SAN Manager **14000** outputs the results. [Step **1340**] Processing continues with step **1300**.

Paragraph [0120] of Yamamoto likewise contains no teaching or suggestion of an SCC list "comprising a list of devices authorized to participate in said secure network." At most this passage teaches a list that contains information about devices that are connected to the network,

without regard to whether they are authorized or not, and contains no information about devices that are not connected to the network, again without regard to whether they are authorized or not.

> **[0302]** A common network management interface **3420** at the Network Management Layer provides an interface between: (a) applications **3405** (such as a GUI), customer services **3410**, and other NMSs/OSSs **3415**, and (b) a configuration manager **3425**, connection manager **3430**, **3440**, fault manager **3445**, and performance manager **3450**, which may share common resources/services **3435**, such as a database server, which uses an appropriate database interface, and a topology manager **3440**. The database server or servers may store information for the managers **3425**, **3430**, **3445** and **3450**. The interface **3420** may provides a rich set of client interfaces that include RMI, EJB and CORBA, which allow the carrier to integrate the NMS with their systems to perform end-to-end provisioning and unify event information. Third-party services and business layer applications can also be easily integrated into the NMS via this interface. The interface **3420** may be compatible with industry standards where possible.

Paragraph [0302] of Battou also lacks any disclosure of an SCC list "comprising a list of devices authorized to participate in said secure network."

> **[0306]** The configuration manager **3425** provides a switch level view of the NMS, and may provide functions including provisioning of the Node Managers and LCMs, status and control, and installation and upgrade support. The configuration manager **3425** may also enable the user, e.g., via the GUI **3405**, to graphically identify the state of the system, boards, and lower level devices, and to provide a point and click configuration to quickly configure ports and place them in service. The configuration manager may collect switch information such as IP address and switch type, as well as card-specific information such as serial number and firmware/software revision.
>
> **[0307]** The connection manager **3430** provides a way to view existing light path connections between OTSs, including connections within the OTS itself, and to create such connections. The connection manager **3430** supports simple cross connects as well as end-to-end connections traversing the entire network. The user is able to dictate the exact path of a light path by manually specifying the ports and cross connects to use at an OTS. Or, the user may only specify the endpoints and let the connection manager set up the connection automatically. Generally, the endpoints of a connection are OA ports, and the intermediate ports are TP ports. The user may also select a wavelength for the connection. The types of connections supported include Permanent Optical Circuit (POC), Switched Optical Circuit (SOC), as well as Smart Permanent Optical Circuit (SPOC). SOC and SPOC connections are routed by the network element routing and signaling planes. SOC connections are available for viewing only.

Finally, ¶¶ [0306]–[0307] of Battou also fails to teach or suggest anything relating to an SCC list "comprising a list of devices authorized to participate in said secure network." Moreover, this passage also makes abundantly clear that it is talking about telecommunication provider optical fiber networks, and not Fibre Channel networks, thus reinforcing the impropriety of combining Battou with Yamamoto set forth above.

Therefore, the rejection of claim 16 as obvious over Yamamoto in view of Battou is improper and should be reversed.

### E. The Rejection Of Claims 10, 17–24 And 54 As Obvious Over Yamamoto In View Of Battou In Further View Of Zara Is Improper

Claims 10, 17–24, and 54 were rejected under 35 U.S.C. § 103(a) as obvious over Yamamoto in view of Battou and U.S. Pre-Grant Publication 2004/0015957 to Zara ("Zara"). Claim 10 depends (indirectly) from claim 1 and is therefore patentable for at least the reasons set forth above with respect to claim 1. Claims 17–24 and 54 are all independent claims that require, in various combination, one or more of the following limitations: (1) an NCE list substantially as discussed above with respect to claim 1, (2) an SCC list substantially as discussed above with respect to claim 16, and (3) a DCC list substantially as discussed above with respect to claims 5 and 6. This alone provides sufficient reason that the rejection of claims 10, 17–24, and 54 is improper and should be reversed.

Moreover, an additional element found in various claims among 17–24 and 54 is the "MAC list, said MAC list comprising an indication of network endpoints from which management access is acceptable." Examiner concedes that the required MAC list is not present in Yamamoto or Battou and proposes U.S. Pre-grant publication 2004/0015957 by Zara ("Zara") to supply this missing limitation. While Zara does disclose so-called "MAC" addresses, these are *media* access control addresses, which are unique identifiers of network adapters in an Ethernet network. The "MAC list" of the pending claims is a *management* access control list, and has nothing to do with Ethernet MAC addresses. As can be seen from the plain language of the claim the MAC list must indicate the endpoints from which management is acceptable. The MAC address used for intrusion detection in Zara does not even bear passing resemblance to a list of devices from which management access is permitted. Therefore the rejection of claims 17–24 and 54 including this limitation is improper and should be reversed.

Additionally, each of claims 17–24 and 54 incorporate in some way, shape, or form, the exclusive control limitation discussed above with respect to claim 1. For example, claim 17 is drawn to a network configuration entity "configured or adapted to exclusively control a defined set of management functions...." Similarly, claim 18 is drawn to a Fibre Channel switching device ... wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity...." Each of the remaining claims 19–24 and 54 include some variation of this limitation. However, as discussed above, Battou is drawn to a network in which the various functions enumerated in the claims are subject to distributed

control among a plurality of NMS managers. Therefore, Battou fails to disclose the required exclusive control and is inappropriate for combination with other references because it teaches away from Applicant's claimed invention. *See* MPEP § 2143, et seq.

Therefore, each of these claims is patentable for at least the reasons set forth above with respect to the corresponding limitations. The rejection of these claims is therefore improper.

**F. Conclusion**

For at least the reasons stated above, Applicants respectfully submit that all outstanding rejections should be reversed. Additionally, to the extent specific claims have not been addressed, these claims depend from one or more claims that are specifically addressed, and are therefore patentable for at least the same reasons as the claims specifically addressed. Applicants further believe that they have complied with each requirement for an appeal brief.

In the course of the foregoing discussions, Applicants may have at times referred to claim limitations in shorthand fashion, or may have focused on a particular claim element. This discussion should not be interpreted to mean that the other limitations can be ignored or dismissed. The claims must be viewed as a whole, and each limitation of the claims must be considered when determining the patentability of the claims. Moreover, it should be understood that there may be other distinctions between the claims and the prior art which have yet to be raised, but which may be raised in the future.

If any fees are required or have been overpaid, please appropriately charge or credit those fees to Deposit Account Number 501922, referencing docket number 112-0020US.

* * * * *

Respectfully submitted,

/Billy C. Allen III/

May 4, 2009

Billy C. Allen III, Reg. No. 46,147
Wong, Cabello, Lutsch,
Rutherford & Brucculeri, L.L.P.
20333 State Hwy 249, Suite 600
Houston, TX 77070
832-446-2409

Filed Electronically

## VIII. CLAIMS APPENDIX

1. (original) A network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure network comprising a plurality of switching devices, said set of management functions comprising the recognition, operation and succession of the network configuration entity.

2. (original) The network configuration entity of claim 1 further comprising a memory for storing an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity.

3. (original) The network configuration entity of claim 1 wherein said set of management functions further comprise one or more rules for interaction between and among devices in the network.

4. (original) The network configuration entity of claim 1 wherein said set of management functions further comprises device connection controls that indicate port relationships in said secure network

5. (original) The network configuration entity of claim 4 further comprising a memory for storing a DCC list, said DCC list associated with said one or more rules for interaction between and among devices and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network.

6. (original) The network configuration entity of claim 3 further comprising a memory for storing a DCC list, said DCC list associated with said one or more rules for interaction between and among devices and comprising definitions that logically bind each port in said secure network to one or more other ports resident in said said network.

7. (previously presented) The network configuration entity of claim 6 wherein said ports are identified by a unique number.

8. (previously presented) The network configuration entity of claim 7 wherein said unique number is a world-wide-name.

9. (original) The network configuration entity of claim 1 wherein said set of management functions further comprises management access controls that restrict management services to a defined set of endpoints.

10. (original) The network configuration entity of claim 9 further comprising a memory for storing an MAC list, said MAC list comprising an indication of network endpoints from which management access is acceptable.

11. (previously presented) The network configuration entity of claim 9 wherein said network endpoints comprise IP addresses.

12. (previously presented) The network configuration entity of claim 11 wherein said IP addresses are associated with access from SNMP or Telnet or HTTP or API.

13. (previously presented) The network configuration entity of claim 9 wherein said network endpoints comprise uniquely identified device ports.

14. (previously presented) The network configuration entity of claim 9 wherein said network endpoints comprise uniquely identified devices resident in said secure network.

15. (original) The network configuration entity of claim 1 wherein said set of management functions further comprises switch connection controls for designating devices to participate in the secure network.

16. (original) The network configuration entity of claim 15 further comprising a memory for storing an SCC list, said SCC list associated with said switch connection controls and comprising a list of devices authorized to participate in said secure network.

17. (previously presented) A network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, (ii) switch connection controls for designating devices to participate in the secure network, (iii) device connection controls that indicate port relationships in said secure network, and (iv) management access controls that restrict management services to a defined set of endpoints, said network configuration entity comprising:

a processor; and

a memory for storing

an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity,

an SCC list, said SCC list comprising an indication of each device allowed to participate in said secure network,

a DCC list, said DCC list associated with said one or more rules for interaction between and among devices and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network, and,

a MAC list, said MAC list comprising an indication of network endpoints from which management access is acceptable.

18. (original) A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, (ii) switch connection controls for designating devices to participate in the secure network, (iii) device connection controls that indicate port relationships in said secure network, and (iv) management access controls that restrict management services to a defined set of endpoints, said Fibre Channel switching device comprising:

a processor; and

a memory for storing

an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity,

an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network,

a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network, and,

a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable.

19. (original) A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, and (ii) switch connection controls for designating devices to participate in the secure network, said Fibre Channel switching device comprising:

a processor; and

a memory for storing

an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity, and

an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network.

20. (original) A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, and (ii) device connection controls that indicate port relationships in said secure network, said Fibre Channel switching device comprising:

a processor; and

a memory for storing

an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity, and

a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network.

21. (original) A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity, and (ii) management access controls that restrict management services to a defined set of endpoints, said Fibre Channel switching device comprising:

a processor; and

a memory for storing

an NCE list, said NCE list associated with said recognition, operation and succession of the network configuration entity and comprising an indication of each device in the network that may operate as said network configuration entity, and

a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable.

22. (original) A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) switch connection controls for designating devices to participate in the secure network, and (ii) device connection controls that indicate port relationships in said secure network, said Fibre Channel switching device comprising:

a processor; and

a memory for storing

an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network, and

a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network.

23. (original) A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) switch connection controls for designating devices to participate in the secure network, and (ii) management access controls that restrict management services to a defined set of endpoints, said Fibre Channel switching device comprising:

a processor; and

a memory for storing

an SCC list, said SCC list associated with said switch connection controls and comprising an indication of each device allowed to participate in said secure network, and

a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable.

24. (original) A Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management functions is controlled throughout said secure network by a network configuration entity, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) device connection controls that indicate port relationships in said secure network, and (ii) management access controls that restrict management services to a defined set of endpoints, said Fibre Channel switching device comprising:

a processor; and

a memory for storing

a DCC list, said DCC list associated with said device connection controls and comprising definitions that logically bind a port on the network configuration entity, to one or more other ports resident in the secure network, and,

a MAC list, said MAC list associated with said management access controls and comprising an indication of network endpoints from which management access is acceptable.

25. (original) A network comprising a network configuration entity and one or more other entities, said network configuration entity having network-wide control over a defined set of management functions, said set of management functions comprising:

the recognition, operation and succession of the network configuration entity;

one or more rules for interaction between and among entities in the network;

one or more rules governing management level access to the network; and

one or more rules governing management level access to one or more entities.

26. (original) The network of claim 25 wherein said function of recognition, operation and succession of the network configuration entity is associated with a list of network devices that are eligible to become equivalent to said network configuration entity.

27. (original) The network of claim 25 wherein the network configuration entity has exclusive control over one or more of said management functions.

28. (original) The network of claim 25 further comprising one or more back-up network configuration entities.

29. (original) The network of claim 25 wherein each of said security and management functions corresponds with a data structure in a memory.

30–53 (cancelled)

54. (original) A method of securing a network having a Fibre Channel switching device configured or adapted to operate in a secure network wherein a defined set of management function is controlled throughout said secure network by a network configuration entity, said method comprising the steps of:

controlling the recognition, operation and succession of the network configuration entity by designating an NCE list comprising an indication of each device in the network that may operate as said network configuration entity;

designating a unique name for each devices that may participate in the secure network;

indicating port relationships in said secure network to specifically delineate a list of unique names for ports that any given port may communicate with; and

restricting management access to a pre-defined set of access methods.

## IX. EVIDENCE APPENDIX

None.

## X. RELATED PROCEEDINGS APPENDIX

None.